

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:)
)
Hideto YASUDA et al.)
) Group Art Unit:
Serial No.: NEW)
) Examiner:
Filed: April 4, 2000)



For: USER AUTHENTICATION APPARATUS, METHOD OF USER
AUTHENTICATION, AND STORAGE MEDIUM THEREFOR

**SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN
APPLICATION IN ACCORDANCE
WITH THE REQUIREMENTS OF 37 C.F.R. §1.55**

*Honorable Commissioner of Patents and Trademarks
Washington, D.C. 20231*

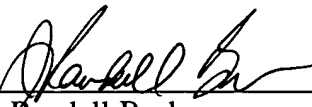
Sir:

In accordance with the provisions of 37 C.F.R. §1.55, the applicant(s) submit(s)
herewith a certified copy of the following foreign application:

Japanese Patent Application No. 11-198061
Filed: July 12, 1999

It is respectfully requested that the applicants be given the benefit of the foreign filing
date as evidenced by the certified papers attached hereto, in accordance with the requirements
of 35 U.S.C. §119.

Respectfully submitted,
STAAS & HALSEY LLP

By: 
J. Randall Beckers
Registration No. 30,358

700 11th Street, N.W., Ste. 500
Washington, D.C. 20001
(202) 434-1500

Date: 4/4/2000

日 本 国 特 許 庁

PATENT OFFICE
JAPANESE GOVERNMENT

Jc586 U.S. PTO
09/542908
04/04/00

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年 7月12日

出 願 番 号
Application Number:

平成11年特許願第198061号

出 願 人
Applicant (s):

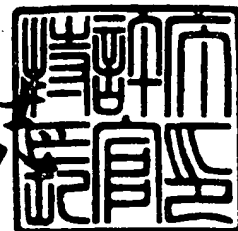
富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

1999年 8月26日

特許庁長官
Commissioner,
Patent Office

伴佐山建



【書類名】 特許願

【整理番号】 9950479

【提出日】 平成11年 7月12日

【あて先】 特許庁長官殿

【国際特許分類】 G06F 15/00

【発明の名称】 認証制御装置、認証制御システムおよび認証制御方法並びに記録媒体

【請求項の数】 10

【発明者】

 【住所又は居所】 神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内

 【氏名】 安田 英人

【発明者】

 【住所又は居所】 長野県松本市深志1丁目1番15号 株式会社富士通パソコンラボ内

 【氏名】 大澤 智人

【特許出願人】

 【識別番号】 000005223

 【氏名又は名称】 富士通株式会社

【代理人】

 【識別番号】 100072590

 【弁理士】

 【氏名又は名称】 井桁 貞一

 【電話番号】 044-754-3035

【手数料の表示】

 【予納台帳番号】 011280

 【納付金額】 21,000円

【提出物件の目録】

 【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9704486

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証制御装置、認証制御システムおよび認証制御方法並びに記録媒体

【特許請求の範囲】

【請求項 1】 利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、

前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する設定部と、

を備える認証制御装置。

【請求項 2】 利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、

前記照合結果に応じて、前記記録媒体に記録されている対象システムに関する認証情報を利用者により入力された新たな認証情報への変更を制御する変更制御部と、

前記記録媒体に記録された認証情報の変更に同期して、前記入力された新たな認証情報を用いてシステムが保持している認証情報を変更する変更処理部と、

を備える認証制御装置。

【請求項 3】 利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、

前記照合結果に応じて、前記記録媒体に記録されている複数の証明書の中から所望の証明所の読み出しを指示する指示部と、

前記記録媒体から読み出される前記指示された証明書をシステムに供給する供給部と、

を備える認証制御装置。

【請求項 4】 複数のシステムにそれぞれ対応する認証情報と固有の識別情報とを保持する記録媒体と、前記記録媒体に保持されている認証情報をシステムでの認証に用いる装置からなる認証制御システムであり、

前記装置は、

利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、

前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する設定部とからなる、

認証制御システム。

【請求項 5】 複数のシステムにそれぞれ対応する認証情報と固有の識別情報とを保持する記録媒体と、前記記録媒体に保持されている認証情報をシステムでの認証に用いる装置からなる認証制御システムであり、

前記装置は、

利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、

前記照合結果に応じて、前記記録媒体に記録されている対象システムに関する認証情報を利用者により入力された新たな認証情報への変更を制御する変更制御部と、

前記記録媒体に記録された認証情報の変更に同期して、前記入力された新たな認証情報を用いてシステムが保持している認証情報を変更する変更処理部とからなる、

認証制御システム。

【請求項 6】 利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報とを照合し、

前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち対象システムに関する認証情報を読み出し、

前記読み出された認証情報を認証処理の入力情報として設定する、

認証制御方法。

【請求項 7】 利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合し、

前記照合結果に応じて、前記記録媒体に記録されている対象システムに関する認証情報を利用者により入力された新たな認証情報へ変更し、

前記記録媒体に記録された認証情報の変更に同期して、前記入力された新たな認証情報を用いてシステムが保持している認証情報を変更する、
認証制御方法。

【請求項 8】 認証処理に用いられる認証情報を記録する記録媒体であって、
外部と情報を授受する送受信部と、
システムを特定するシステム識別情報と該システム識別情報に対応付けられた認証情報との組を複数記録すると共に媒体固有の情報を記録する記録部と、
外部から供給される情報と前記固有情報の照合を行う照合部と、
前記照合結果に応じて前記認証情報を外部に供給する処理部と、
を備える記録媒体。

【請求項 9】 コンピュータに、
利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する手順と、
前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する手順と、
を実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 10】 コンピュータに、
利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する手順と、
前記照合結果に応じて、前記記録媒体に記録されている対象システムに関する認証情報を利用者により入力された新たな認証情報への変更を制御する手順と、
前記記録媒体に記録された認証情報の変更に同期して、前記入力された新たな認証情報を用いてシステムが保持している認証情報を変更する手順と、
を実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、装置やシステム、サービスなどの利用を許可するために行われる利用者認証に関するものである。

【0002】

近年、ネットワークの整備やパーソナルコンピュータ、通信装置などのハードウェアが安価になったことから、家庭や企業内さらには屋外などの様々な場所において誰でもインターネットを利用した電子メールの送受信やWWW (World Wide Web) 閲覧などが簡単にできるような環境になってきている。

【0003】

また、企業においては、イントラネットやエクストラネットにより業務の迅速化、効率化を図っており、従来のメインフレームを中心としたホスト集中型の業務システムに加え、ネットワークを利用してクライアント/サーバ型の業務システムを構築し、運用を行っている。

【0004】

上述のように、家庭や企業において様々なシステムを誰でも利用することが可能となっているが、このようなシステムやサービスにおいては、これらを利用する際に利用者固有のIDとパスワードを入力させ、その入力情報を使用して利用資格があるか否かを判断する認証処理が通常行われている。

【0005】

さらに、パーソナルコンピュータのオペレーティングシステムにおいても、利用者を制限するためや利用者に応じて各種環境設定を変えるために、IDとパスワードを用いた認証処理が適用されるようになっている。

【0006】

【従来の技術】

このように、家庭や屋外、企業内において様々なシステムやサービス（以下、総称してシステムとする）を利用するために、利用者は各システムに対応するIDとパスワードの組を複数記憶しておく必要がある。

【0007】

利用するシステムの数が少なければ利用者はIDとパスワードを記憶しておくことが可能であるが、複数のシステムを利用する利用者はシステムの数が多くなればIDとパスワードを忘却してしまうという事態に陥ってしまう。

【0008】

このIDとパスワードを忘却することでシステムを利用できなくなるという状況を避けるため、利用者の多くは手帳などに各システム毎のIDとパスワードをメモし、認証処理の際に手帳を見て得られるIDとパスワードを入力するというシステムの利用形態をとっているのが一般的である。

【0009】

また、企業内においては、従業員番号情報を記録した磁気カードを従業員に配布し、その磁気カードを使用して認証処理を行うというシステムの運用形態をとることも行われている。

【0010】

他の従来技術として、信頼度を強化し、必要十分な認証を可能とする特開平7-64911号がある。

【0011】

この公開公報においては、1つのホストコンピュータとそれに接続される複数の端末で構成されるシステムにおいて、ICカードや磁気カードに複数の個人認証データ（識別情報、パスワード、筆跡、指紋など）を記憶させておき、端末には複数の個人認証データを入力できるよう、キーボードやタブレット、磁気カード読取部、ICカード読取部を備え、それらの内のいくつかを選択して複数の個人認証データを入力し、照合することが開示されている。

【0012】

【発明が解決しようとする課題】

上述のように、認証処理の際に、手帳にメモしたIDとパスワードを見て入力するという利用形態においては、手帳の内容を他人に見られIDとパスワードが漏れてしまい、システムが不正利用されるという問題が発生している。

【0013】

また、磁気カードを用いる認証処理は磁気カードを読取装置で読ませるだけと

いう利用者による操作が簡易であるという利点があるが、本来の所有者以外の他人が磁気カードを読取装置に読ませることだけで認証が行われてしまい、セキュリティが脆弱でシステムへの不正アクセスを防止できない。

【0014】

さらに、特開平 7-64911 号においては、複数の個人認証データを使用するということでセキュリティの効果は大きいが、1つのシステムに対するセキュリティは向上できるものの複数のシステムに対するセキュリティの向上、利用者による認証操作の簡易化は想定されているものではない。

【0015】

本発明は、複数のシステムに対する利用者の操作の簡易化、複数のシステムを利用する環境におけるセキュリティ向上のための認証制御装置、認証制御システム、記録媒体を提供することを目的とする。

【0016】

【課題を解決するための手段】

上記目的を達成するために、本発明では、利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する設定部とで装置を構成する。

【0017】

また、利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、前記照合結果に応じて、前記記録媒体に記録されている対象システムに関する認証情報を利用者により入力された新たな認証情報への変更を制御する変更制御部と、前記記録媒体に記録された認証情報の変更と同期して、前記入力された新たな認証情報を用いてシステムが保持している認証情報を変更する変更処理部とで装置を構成する。

【0018】

また、利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部と、前記照合結果に応じて、前記記録媒体

に記録されている複数の証明書の中から所望の証明所の読み出しを指示する指示部と、前記記録媒体から読み出される前記指示された証明書をシステムに供給する供給部とで装置を構成する。

【0019】

また、本発明の特徴を備えた上記装置と上記記録媒体からなるシステムとして構成してもよい。

【0020】

また、上記記録媒体を、外部と情報を授受する送受信部と、システムを特定するシステム識別情報と該システム識別情報に対応付けられた認証情報との組を複数記録すると共に媒体固有の情報を記録する記録部と、外部から供給される情報と前記固有情報の照合を行う照合部と、前記照合結果に応じて前記認証情報を外部に供給する処理部とで構成する。

【0021】

さらに、コンピュータである装置を制御するプログラムを、利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する手順と、前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する手順とを実行させるよう構成する。

【0022】

また、コンピュータである装置を制御するプログラムを、利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する手順と、前記照合結果に応じて、前記記録媒体に記録されている対象システムに関する認証情報を利用者により入力された新たな認証情報への変更を制御する手順と、前記記録媒体に記録された認証情報の変更と同期して、前記入力された新たな認証情報を用いてシステムが保持している認証情報を変更する手順とを実行させるよう構成する。

【0023】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

【0024】

本発明の実施形態においては、ネットワークを介して接続されるクライアント／サーバシステムを例として説明する。なお、本例のようにクライアント／サーバシステムではなく、メインフレームを中心としたホスト集中型のシステムであっても構わない。

【0025】

図1は、本発明のシステム構成図である。

【0026】

図1に示されるように、クライアント1はネットワーク3を介してサーバ2に接続される。そして、クライアント1はサーバ2にアクセスし、サーバ2上のアプリケーションソフトを利用した業務処理や、サーバ2からデータのダウンロード処理などを行う。

【0027】

図2は、クライアント1であるコンピュータの概略構成を示す図である。

【0028】

クライアント1は、主に、CPU4、RAM5、HDD（ハードディスクドライブ）6、CD-ROMドライブ7、FDD（フロッピーディスクドライブ）8、NCU（ネットワーク制御ユニット）9、ディスプレイ10、キーボード11、ICカードリーダーライター12から構成される。

【0029】

図中、CPU4はプログラムにより各種処理、制御を実行するものであり、本発明のプログラムによる各種処理、制御においても使用される。

【0030】

また、RAM5はCPU4による各種処理や制御のための一時的なデータの保持や、ディスプレイ10に表示するためのデータを保持するために使用される。

【0031】

ハードディスクドライブ6およびフロッピーディスクドライブ8は、プログラムや制御データを不揮発性の記録媒体（ハードディスクやフロッピーディスク14）に記録したり、該記録媒体からプログラムや制御データを読み出すためのデ

バイスである。

【0032】

CD-ROMドライブ7はCD-ROM13に記録されたプログラムや制御データを読み出すためのデバイスである。

【0033】

ネットワーク制御ユニット9は、ネットワーク3に接続し、ネットワーク3を介して他の装置とのデータのやり取りを行うものである。このネットワーク制御ユニット9によりネットワーク3を介してサーバ2とのデータの授受が可能となる。

【0034】

このネットワーク制御ユニットは、モデムであってもいいし、LANカードであってもよい。

また、サーバ2からのプログラム、データのダウンロードやサーバ2が提供するサービスを受けるためにも使用できる。

【0035】

クライアント1で動作する本発明のプログラムはCD-ROM13やフロッピーディスク14などに記録されているものをそれぞれCD-ROMドライブ7やフロッピーディスクドライブ8などによって読み取り、ハードディスクドライブ6の記録媒体にインストールされるものである。

【0036】

また、上記本発明のプログラムをネットワーク制御ユニット9によりネットワークを介して他の装置からダウンロードしてハードディスクドライブ6の記録媒体に格納するようにしてもよい。

【0037】

このようにしてハードディスクドライブ6の記録媒体に格納された本発明のプログラムは、実行指示によりRAM5にロードされ、CPU4を制御して本発明の各構成要件をコンピュータであるクライアントにて実現するよう動作する。

【0038】

上記のように、本発明のプログラムを一旦ハードディスクドライブ6の記録媒

体に格納するという形態ではなく、ネットワークを介して他の装置からダウンロードしてRAM5に直接展開するよう構成してもよい。

【0039】

ディスプレイ10はRAM5に保持されるデータを画面上に表示するためのものである。

【0040】

キーボード11は主にユーザが文字情報を入力するために用いるもの入力デバイスである。なお、図示されていないが、ディスプレイ10の画面上に表示されるマウスカーソルを操作するためのマウスも接続されている。

【0041】

ICカードリーダライタ12はICカード15（スマートカードともいう）からの情報の読み出し、および情報の書き込みを行うためのデバイスである。このICカード15は例えばプラスチックのカード上に集積回路（IC）が設けられたものであり、この集積回路はICカードリーダライタ12と電氣的に接続するための接点部と、各種処理を行う処理部と、情報を記録する記録部を備える。

【0042】

本例でのICカードリーダライタ12とICカード15は物理的に接触して情報の読み出しおよび書きこみを行うものを説明するが、非接触型のICカードリーダライタとICカードもあり、そちらを利用することも可能である。

【0043】

上記クライアント1と同様に、本発明の他のプログラムはこのICカード15の記録部に記録されており、ICカード15の処理部を制御して本発明の処理を行うよう動作する。

【0044】

以下、本発明のプログラムで行われる処理について詳細に説明する。

【0045】

まず、例として、LOGON画面を表示し、IDとパスワードを入力させてユーザ認証を行うシステムでの処理について図3～図6を用いて説明する。ここでのLOGON画面は、OSの起動時やサーバによるサービスを提供する初期段階

などに表示されるものである。

【0046】

図3および図4は、本実施の形態における認証処理を説明するための処理フローチャートである。

【0047】

また、図5および図6は上記認証処理での画面表示の遷移を示す図である。

【0048】

まず、認証情報を入力するための画面表示であるLOGON画面が表示されると(図5(a))、個人識別情報(以下、PINと称する)を入力させるための画面を表示する。(ステップS11、図5(b))

このPINの入力画面の表示は、前記LOGON画面が表示されたことを検出してそれをトリガとして表示するように構成してもよいし、図示しない画面表示指示ボタンが操作されたことを検出して表示するように構成してもよい。

【0049】

上記PINの入力画面が表示された状態においてキャンセル指示がされると(ステップ12)、本認証処理をキャンセルして終了する。一方、PIN入力画面にユーザがキーボード11を用いてPINを入力して入力完了指示を行うと、入力されたPINはICカード15に供給される。(ステップS13)

ICカード15においては、クライアント本体から供給されるPINと記録部に記録されているPINとの照合を行う。(ステップS14)

ステップS14の照合の結果、ユーザによって入力されたPINが記録部に記録されているPINが一致しない場合、クライアント本体にその不一致の旨の情報を送信する。

【0050】

クライアント本体はICカード15から前記不一致の旨の情報を受信すると、ユーザに入力されたPINが正しくないことをメッセージとして画面上に表示する。(ステップS15、S16)

また、ICカード15はユーザによって入力されたPINと記録部に記録されているPINが一致した場合には、クライアント本体にその一致の旨の情報を送

信し、その後のクライアント本体からのアクセスを許可する状態に設定する。

【0051】

クライアント本体（CPU4）はICカード15からPINが一致する旨の情報を受信すると、ICカード15に記録されているアプリケーション名の一覧を要求する。ICカード15はその要求を受信して、記録部に記録されている各レコードの情報からアプリケーション名に関する情報を読み出し、クライアント本体に供給する。

【0052】

クライアント本体はICカード15からアプリケーション名に関する情報を受信し、それを選択候補として画面上に表示する。（ステップS17、図6（c））

ユーザは現在のシステム（アプリケーション）に応じたアプリケーション名を選択し、選択確定操作を行う。（ステップS18）

ユーザによってアプリケーション名が選択されると、選択されたアプリケーション名に関する情報をICカード15に供給し、該選択アプリケーションに対応する認証情報の読み出しを要求する。このとき、画面上に表示していた選択候補の一覧は消去する。

【0053】

ICカード15はアプリケーション名に関する情報とそれに対応する認証情報の読み出し要求を受信し、供給されるアプリケーション名に関する情報に基づき記録部の各レコードから要求に合致する情報を読み出してクライアント本体に供給する。

【0054】

クライアント本体はICカード15から供給された認証情報を受信し、その認証情報をLOGON画面の所定の入力フィールドに設定する。（図6（d））

入力フィールドに認証情報が設定されると、ユーザは確定操作を行う。

【0055】

認証情報が確定されると、その認証情報がシステムに供給され認証処理（照合処理）が行われる。（ステップS19）

ステップ S 19 による認証処理の結果、入力された認証情報と一致する情報があれば LOGON 処理を行う。(ステップ S 20)

また、入力された認証情報に一致する情報がなければ、ステップ S 17 で表示したアプリケーション名の一覧を画面上に表示して、再び上記ステップ S 18 ～ S 20 の処理を行う。

【0056】

以上のように、ユーザが PIN を入力し、IC カード 15 から読み出され画面上に表示されるアプリケーション名一覧の中から所望のものを選択するだけで、該アプリケーションに関する認証情報を入力フィールドに設定することが可能になる。

【0057】

従って、ユーザは 1 つの識別情報を覚えておくだけで、複数のシステムを利用することが可能となる。また、IC カードの記録部に記録されている情報はその IC カードの処理部のみが読み出し可能なため、他人による認証情報への直接アクセスすることによる盗聴を防止することが可能となる。

【0058】

上記例では認証情報を入力させるログイン画面を表示するシステム(アプリケーション)について説明しているが、これに限定されるものでなく、画面焼き付き防止のためのスクリーンセーバからの復帰時に表示されるパスワード入力画面にも本発明は適用することができる。すなわち、利用者 ID やパスワードを入力する状態になるものに関して本発明は応用することが可能である。

【0059】

また、上記例ではユーザがアプリケーション名の一覧から所望のものを選択する構成をとっているが、現アプリケーション(システム)の識別情報が取得できる場合、IC カード 15 からアクセス許可を受信した後、該識別情報を基に IC カード 15 に該アプリケーションの認証情報を要求するように構成してもよい。これにより、アプリケーション名の一覧を画面表示させ、ユーザに選択させるという操作を削減することができる。

【0060】

次に、認証処理に使用される認証情報を変更する際に、システム（以下、アプリケーションともいう）が管理している認証情報と IC カードに記録された認証情報の同期をとる処理を説明する。

【0061】

図 7 および図 8 は、本実施の形態における認証情報の変更処理を説明するための処理フローチャートである。

【0062】

また、図 9 は上記変更処理での画面表示例を示す図である。

【0063】

まず、パスワードを変更するための入力画面が表示されると、個人識別情報（PIN）を入力させるための画面を表示する。（ステップ S 2 1）

この PIN の入力画面の表示は、システムで用意している既存のパスワード変更入力画面が表示されたことを検出してそれをトリガとして表示するように構成してもよいし、専用のパスワード変更入力画面を表示するように構成してもよい。

【0064】

上記 PIN の入力画面が表示された状態においてキャンセル指示がされると（ステップ 2 2）、本変更処理をキャンセルして終了する。一方、PIN 入力画面にユーザがキーボード 11 を用いて PIN を入力して入力完了指示を行うと、入力された PIN は IC カード 15 に供給される。（ステップ S 2 3）

IC カード 15 においては、クライアント本体から供給される PIN と記録部に記録されている PIN との照合を行う。（ステップ S 2 4）

ステップ S 2 4 の照合の結果、ユーザによって入力された PIN が記録部に記録されている PIN が一致しない場合（ステップ S 2 5）、クライアント本体にその不一致の旨の情報を送信する。

【0065】

クライアント本体は IC カード 15 から前記不一致の旨の情報を受信すると、ユーザに入力された PIN が正しくないことをメッセージとして画面上に表示する。（ステップ S 2 6）

また、ICカード15はユーザによって入力されたPINと記録部に記録されているPINが一致した場合には、クライアント本体にその一致の旨の情報を送信し、その後のクライアント本体からのアクセスを許可する状態に設定する。

【0066】

クライアント本体(CPU4)はICカード15からPINが一致する旨の情報を受信すると、図9のパスワードの入力フィールドへの情報入力を有効にする。

【0067】

ユーザは有効になったパスワードの入力フィールドへ古いパスワード、新しいパスワード、確認のための新しいパスワードをそれぞれ入力し、入力確定操作を行う。

【0068】

パスワード変更のための入力情報が確定されると、システムがパスワードの変更処理を行うと共に、クライアント本体(CPU4)はICカード15に対し、ICカード15に記録されているアプリケーション名の一覧を要求する。ICカード15はその要求を受信して、記録部に記録されている各レコードの情報からアプリケーション名に関する情報を読み出し、クライアント本体に供給する。

【0069】

クライアント本体はICカード15からアプリケーション名に関する情報を受信し、それを選択候補として画面上に表示する。(ステップS27)

ユーザは現在のシステム(アプリケーション)に応じたアプリケーション名を選択し、選択確定操作を行う。(ステップS28)

ユーザによってアプリケーション名が選択されると、選択されたアプリケーション名に関する情報と共に、変更要求としてユーザによって入力されたパスワードに関する各情報をICカード15に供給する。このとき、画面上に表示していた選択候補の一覧は消去する。

【0070】

ICカード15は新たなパスワードへの変更要求を受信し、供給されるアプリケーション名に関する情報とパスワードに関する情報に基づき記録部の各レコー

ドから該アプリケーション名に合致するパスワードの情報フィールドを新たなパスワードに書き換える。(ステップ S 29)

また、選択されたアプリケーションに関する情報のパスワードとユーザによって入力された古いパスワードが一致しないなど、現在のシステムに合致しない入力がされた場合には(ステップ S 30)、ステップ S 27 で表示したアプリケーション名の一覧を画面上に表示して、再び上記ステップ S 28 ~ S 30 の処理を行う。

【0071】

このような処理によって、システムおよび IC カード 15 内のパスワードを一度の入力で変更することができる。従って、ユーザによるパスワード変更入力の手間を省くことが可能となる。

【0072】

次に、IC カード 15 に複数の証明書を記録させて利用する例について説明する。

【0073】

この証明書は秘密鍵と呼ばれ、例えば WWW サーバのデータ暗号化で使用され、セキュリティで保護されたページの閲覧などにおいて必要になるものである。

【0074】

図 10 および図 11 は WWW ブラウザによりセキュリティで保護されたページの閲覧時に証明書を使用するときの処理フローチャートである。

【0075】

また、図 12 および図 13 はその Web サイト閲覧時の画面表示の遷移を示す図である。

【0076】

まず、WWW ブラウザでセキュリティで保護されたページの URL を直接入力する、またはリンクを指定すると、ブラウザは証明書の入力を要求する。(図 12 (a))

この要求があると、ユーザは IC カード 15 を IC カードリーダーライタ 12 にセットする。

【0077】

ICカード15がセットされると、個人識別情報（PIN）を入力させるための画面を表示する。（ステップS31，図12（b））

上記PINの入力画面が表示された状態においてキャンセル指示がされると（ステップ32）、本認証処理をキャンセルして終了する。一方、PIN入力画面にユーザがキーボード11を用いてPINを入力して入力完了指示を行うと、入力されたPINはICカード15に供給される。（ステップS33）

ICカード15においては、クライアント本体から供給されるPINと記録部に記録されているPINとの照合を行う。（ステップS34）

ステップS34の照合の結果、ユーザによって入力されたPINが記録部に記録されているPINが一致しない場合、クライアント本体にその不一致の旨の情報を送信する。

【0078】

クライアント本体はICカード15から前記不一致の旨の情報を受信すると、ユーザに入力されたPINが正しくないことをメッセージとして画面上に表示する。（ステップS35，S36）

また、ICカード15はユーザによって入力されたPINと記録部に記録されているPINが一致した場合には、クライアント本体にその一致の旨の情報を送信し、その後のクライアント本体からのアクセスを許可する状態に設定する。

【0079】

クライアント本体（CPU4）はICカード15からPINが一致する旨の情報を受信すると、ICカード15に記録されている証明書名の一覧を要求する。ICカード15はその要求を受信して、記録部に記録されている各証明書名に関する情報を読み出し、クライアント本体に供給する。

【0080】

クライアント本体はICカード15から証明書名に関する情報を受信し、それを選択候補として画面上に表示する。（ステップS37，図13（c））

ユーザは現在のページに応じた証明書名を選択し、選択確定操作を行う。（ステップS38）

ユーザによって証明書名が選択されると、選択された証明書名に関する情報を ICカード 15 に供給し、選択された証明書名に対応するデータの読み出しを要求する。このとき、画面上に表示していた選択候補の一覧は消去する。

【0081】

ICカード 15 は証明書名に関する情報とそれに対応するデータの読み出し要求を受信し、供給される証明書名に関する情報に基づき記録部の各レコードから要求に合致する情報を読み出してクライアント本体に供給する。

【0082】

クライアント本体は ICカード 15 から供給された証明書のデータを受信し、その証明書のデータを用いて認証処理を行う。(ステップ S39)

ステップ S39 による認証処理の結果、正しければセキュリティで保護されたページの表示を行う。(ステップ S40)

また、証明書のデータが正しくなければ、ステップ S37 で表示した証明書名の一覧を画面上に表示して、再び上記ステップ S38～S40 の処理を行う。

【0083】

このように、クライアント本体に証明書のデータを持つのではなく、ICカードのような可搬型の記録媒体に記録しておき、必要に応じてそれから読み出し利用する形態をとることにより、クライアント本体を他人が利用してもこの証明書のデータを記録した記録媒体がなければ、セキュリティで保護されたページの閲覧はできなくなる。

【0084】

よって、高度なセキュリティを実現することが可能となる。

【0085】

最後に、ICカード 15 の記録部に記録されるデータの構造について説明する。

【0086】

図 14 は、ICカードの記録部に記録されるデータの構造を示す図である。

【0087】

1 レコードは、アプリケーション ID、ユーザ ID、パスワード、ドメイン、

拡張の各フィールドからなる。

【0088】

そして、ICカード15の記録部には複数のアプリケーション（システム）のためにそれぞれ対応する複数のレコードが記録されている。

【0089】

アプリケーションIDのフィールドは、アプリケーションを特定するための情報が記録されるものである。これを用いてクライアント本体での選択候補一覧が作成され、また、認証情報を読み出す際のキーとなるものである。

【0090】

ユーザIDのフィールドは、対応するアプリケーションのユーザIDが記録されるものである。

【0091】

パスワードのフィールドは、対応するアプリケーションのユーザIDと対をなすパスワードが記録されるものである。

【0092】

ドメインのフィールドは、上記処理の説明では用いられていないが、サーバにログインする際に用いられる情報が記録されるものである。

【0093】

拡張のフィールドは、拡張情報が次のレコードに続くか否かを示すための情報が記録されるものである。

【0094】

以上、本発明の実施の形態を説明した。

【0095】

なお、本発明は以下の特徴も有する。

（発明1）

利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する制御部であって、該制御部は前記入力識別情報を前記記録媒体に供給する供給部と、

前記記録媒体の照合部による前記入力識別情報と前記固有識別情報との照合結果

を受信する受信部とを備え、

前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する設定部と、

を備える認証制御装置。

(発明 2)

上記発明 1 において、前記照合結果が一致の場合に、前記複数のシステムを選択候補として表示させる表示制御部と、

前記選択候補から対象システムを選択する選択部とを備え、

前記設定部は前記選択された対象システムに関する認証情報を認証処理の入力情報として設定する認証制御装置。

(発明 3)

上記発明 2 において、前記記録媒体に情報の読み出し要求を行う要求部を備え、

前記表示制御部は、前記要求により読み出される前記記録媒体に記録された複数のシステムに関する情報を選択候補として表示させる認証制御装置。

(発明 4)

コンピュータに、

利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報との照合を制御する手順と、

前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち読み出される対象システムに関する認証情報を認証処理の入力情報として設定する手順とを実行させるプログラムであり、さらに前記制御する手順は、

前記入力識別情報を前記記録媒体に供給する手順と、

前記記録媒体の照合部による前記入力識別情報と前記固有識別情報との照合結果を受信する手順と

からなるプログラムを記録したコンピュータ読み取り可能な記録媒体。

(発明 5)

発明 4 において、前記照合結果が一致の場合に、前記複数のシステムを選択候補として表示する手順と、

前記選択候補から対象システムを選択する手順と、

前記記録媒体から読み出される前記選択された対象システムに関する認証情報を認証処理の入力情報として設定する手順と、

をコンピュータに実行させるためのプログラムを記録したコンピュータ読み取り可能な記録媒体。

【0096】

これら発明の構成により、ユーザは 1 つの識別情報を記憶しおくだけで複数のシステムのそれぞれに対応する認証情報を覚えておく必要がなくなる。さらに、識別情報の照合は記録媒体が行い、本装置は照合の要求と照合結果の受信を行う構成であるため、本装置が記録媒体に直接読み出しに行くことを避けることができ、記録媒体に記録されている認証情報のセキュリティが向上する。

【0097】

また、本発明のプログラムも上記処理をコンピュータに実行させることで、同様の作用効果を得ることができる。

【0098】

【発明の効果】

以上のように、本発明によって、ユーザは 1 つの識別情報を覚えておくだけで、複数のシステムを利用することができ、他人による認証情報への直接アクセスすることによる盗聴を防止することが可能となる。

【0099】

また、一度の入力で複数の記録部に記録された認証情報を変更することができるため、ユーザによる認証情報の変更操作の手間を省くことが可能となる。

【0100】

さらに、高度なセキュリティを実現することが可能となる。

【図面の簡単な説明】

【図 1】

本発明のシステム構成図である。

【図 2】

コンピュータの概略構成を示す図である。

【図 3】

本実施の形態における認証処理を説明するための処理フローチャート（その 1）である。

【図 4】

本実施の形態における認証処理を説明するための処理フローチャート（その 2）である。

【図 5】

認証処理での画面表示の遷移を示す図（その 1）である。

【図 6】

認証処理での画面表示の遷移を示す図（その 2）である。

【図 7】

本実施の形態における認証情報の変更処理を説明するための処理フローチャート（その 1）である。

【図 8】

本実施の形態における認証情報の変更処理を説明するための処理フローチャート（その 2）である。

【図 9】

認証情報の変更処理での画面表示例を示す図である。

【図 1 0】

セキュリティで保護されたページの閲覧時に証明書を使用するときの処理フローチャート（その 1）である。

【図 1 1】

セキュリティで保護されたページの閲覧時に証明書を使用するときの処理フローチャート（その 2）である。

【図 1 2】

Web サイト閲覧時の画面表示の遷移を示す図（その 1）である。

【図 1 3】

Web サイト閲覧時の画面表示の遷移を示す図（その 2）である。

【図 1 4】

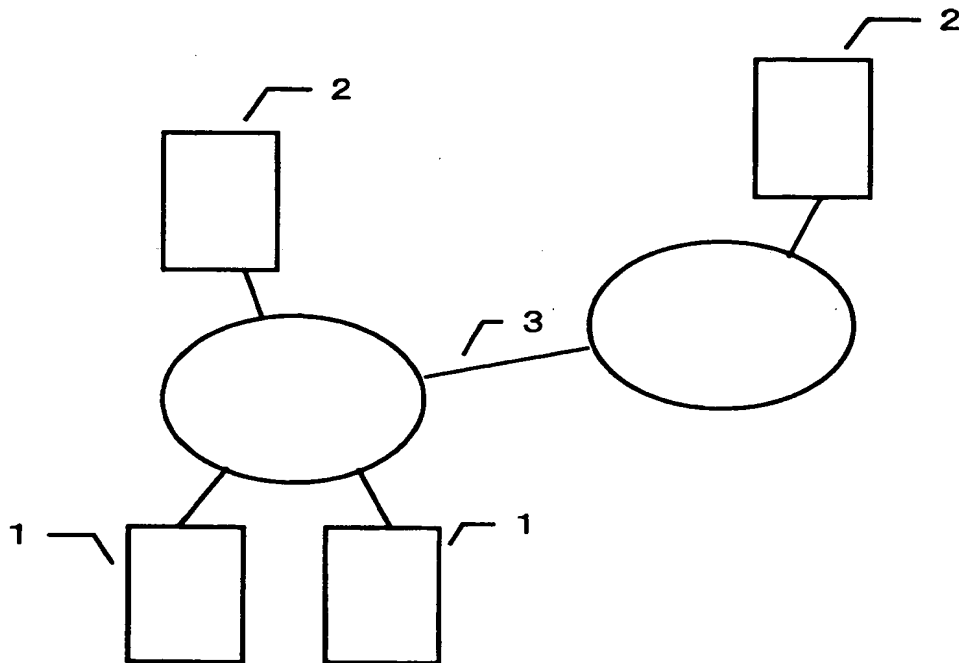
IC カードの記録部に記録されるデータの構造を示す図である。

【符号の説明】

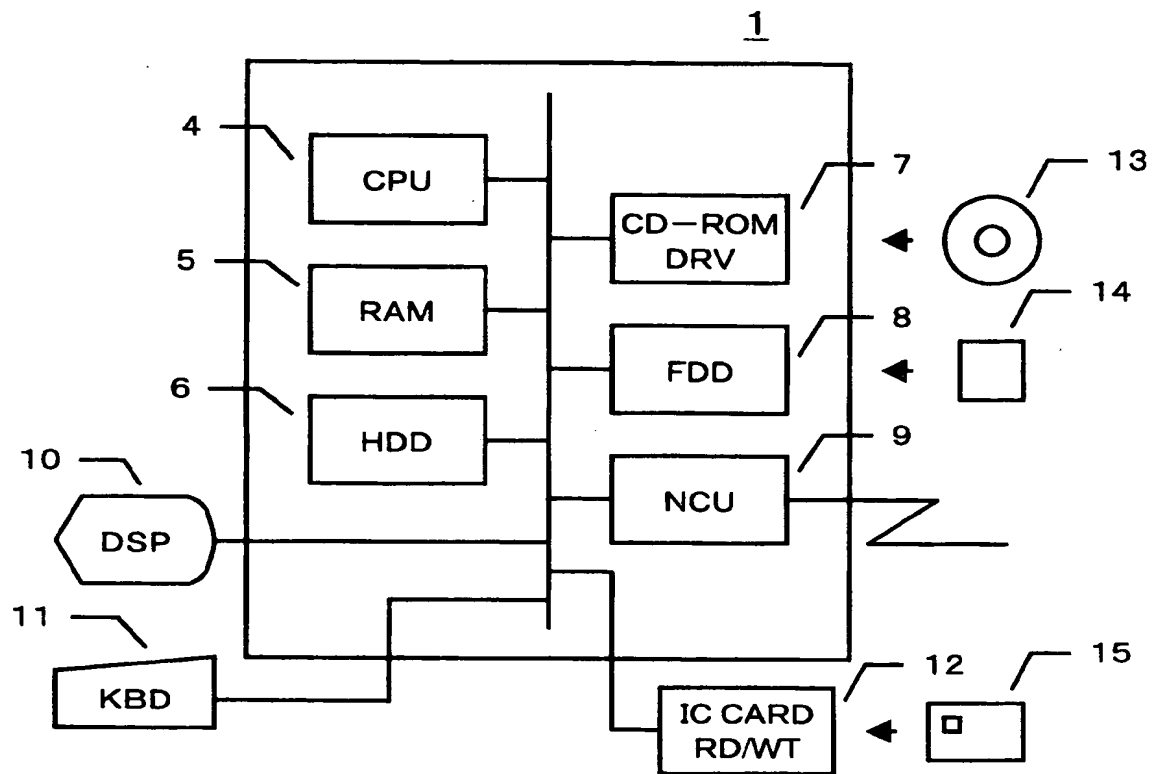
- 1 クライアント
- 2 サーバ
- 3 ネットワーク
- 4 CPU
- 5 RAM
- 6 HDD（ハードディスクドライブ）
- 7 CD-ROM ドライブ
- 8 FDD（フロッピーディスクドライブ）
- 9 NCU（ネットワーク制御ユニット）
- 10 ディスプレイ
- 11 キーボード
- 12 IC カードリーダーライタ 1 2
- 13 CD-ROM
- 14 フロッピーディスク
- 15 IC カード（スマートカード）

【書類名】 図面

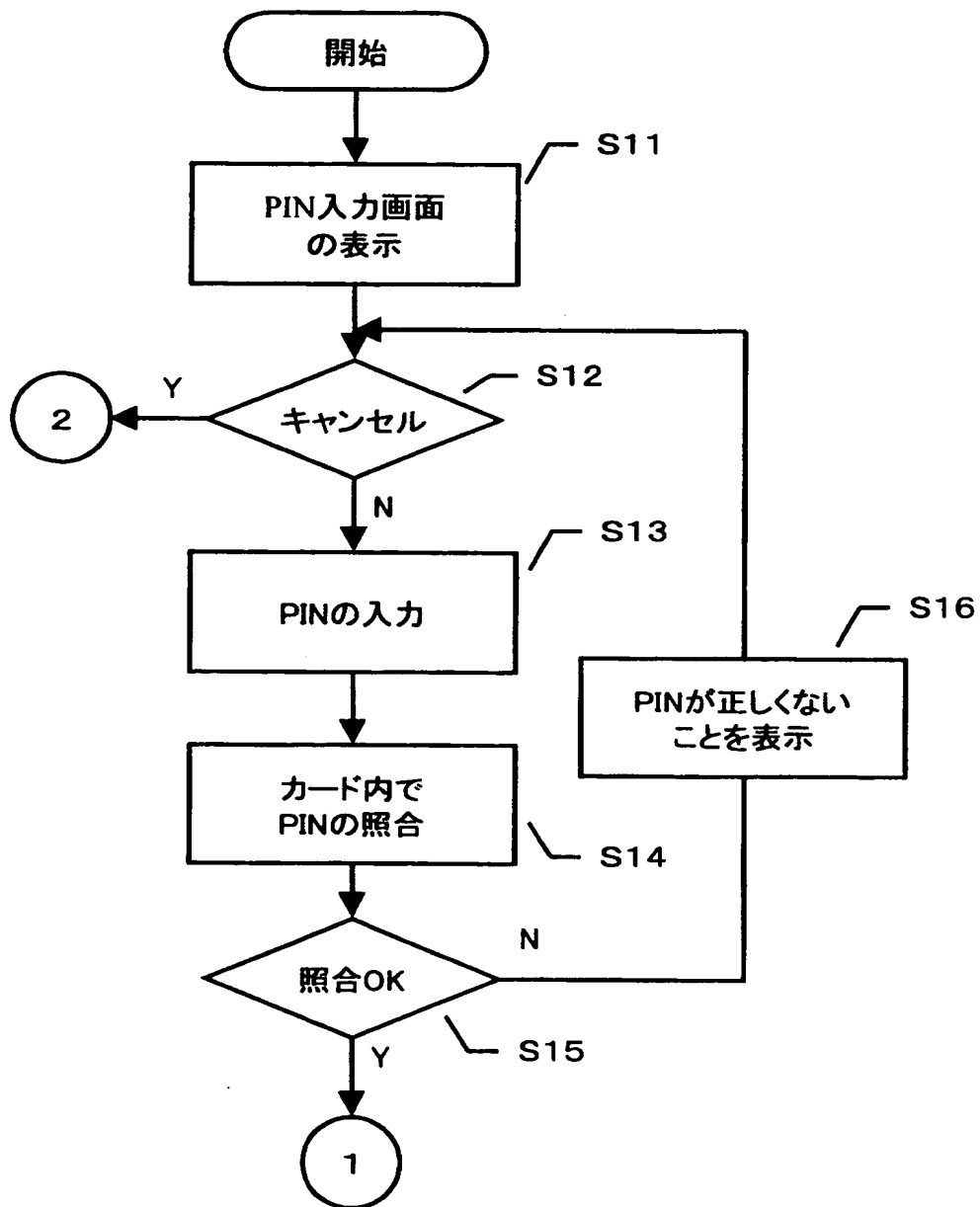
【図 1】



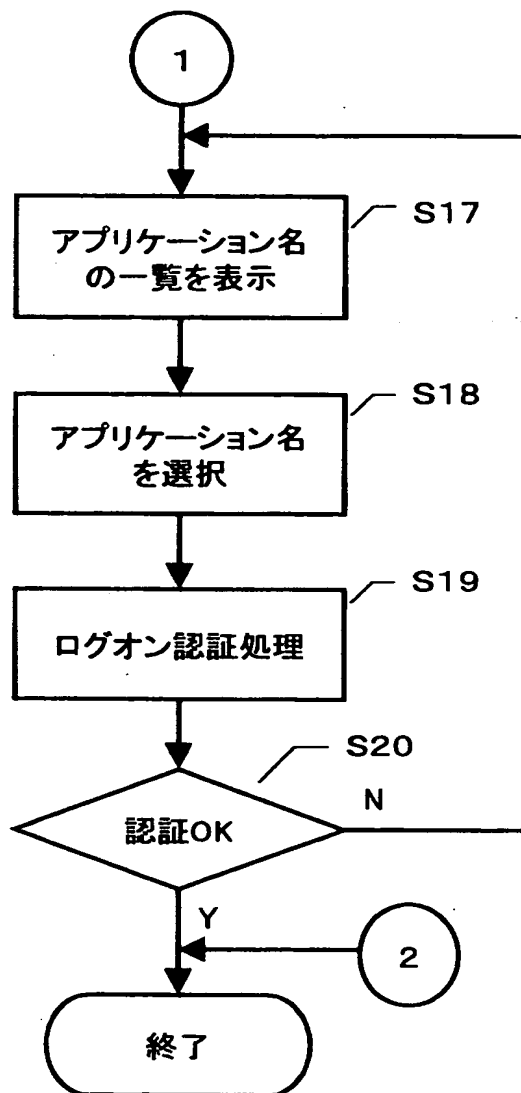
【図 2】



【図 3】



【図 4】



【図 5】

(a)

Diagram (a) illustrates a login screen titled "LOGON画面". It contains two input fields: "ユーザID" (User ID) and "パスワード" (Password). Below these fields are two buttons labeled "OK" and "CAN".

(b)

Diagram (b) illustrates a PIN input screen titled "PIN入力". It contains a single input field for the PIN, represented by a series of asterisks "*****". Below this field are two buttons labeled "OK" and "CAN".

【図 6】

(c)

LOGON画面

ユーザID

パスワード

選択してください。

☒ OS1

☐ サービス1

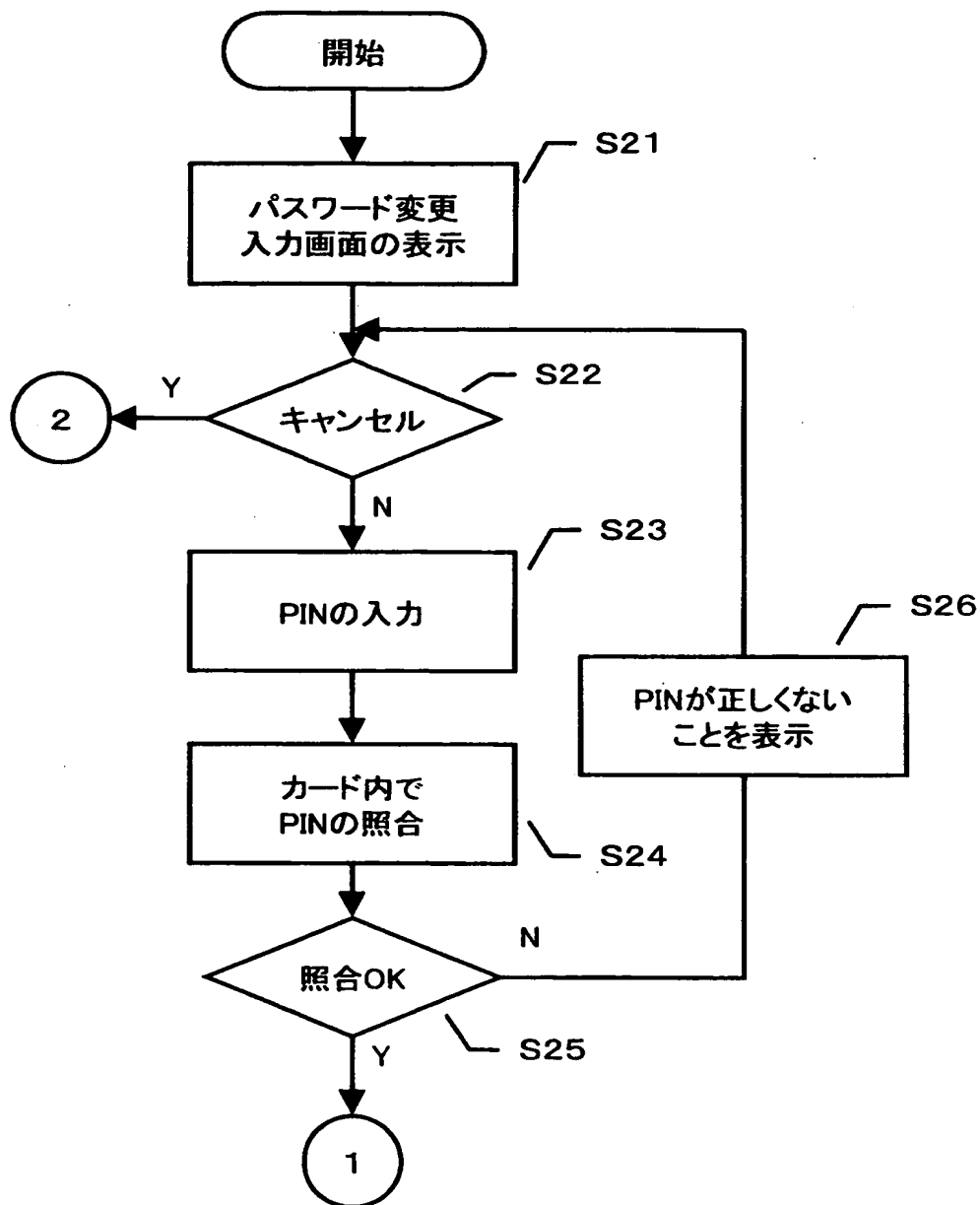
(d)

LOGON画面

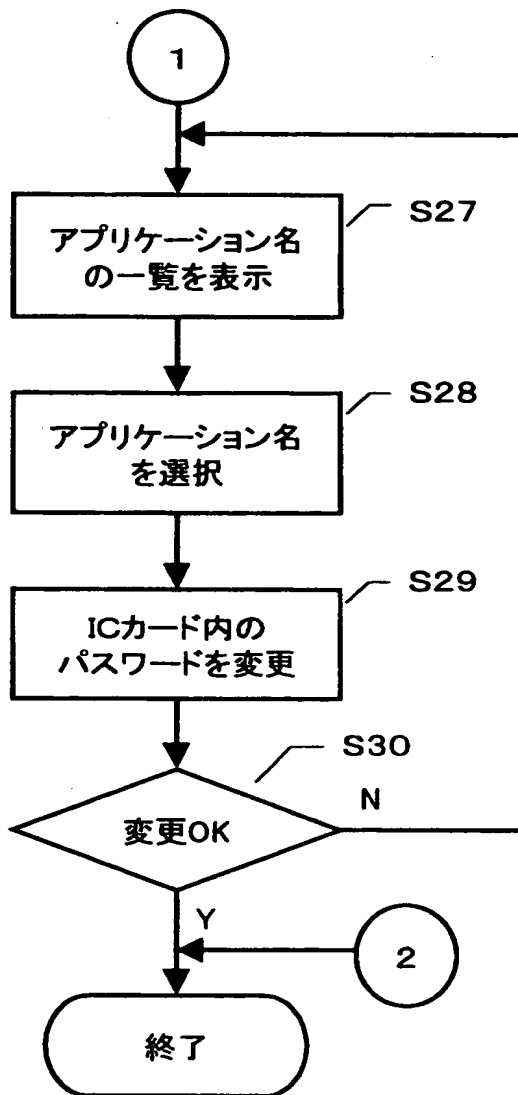
ユーザID

パスワード

【図 7】



【図 8】



【図9】

パスワード変更画面

ユーザID USER1

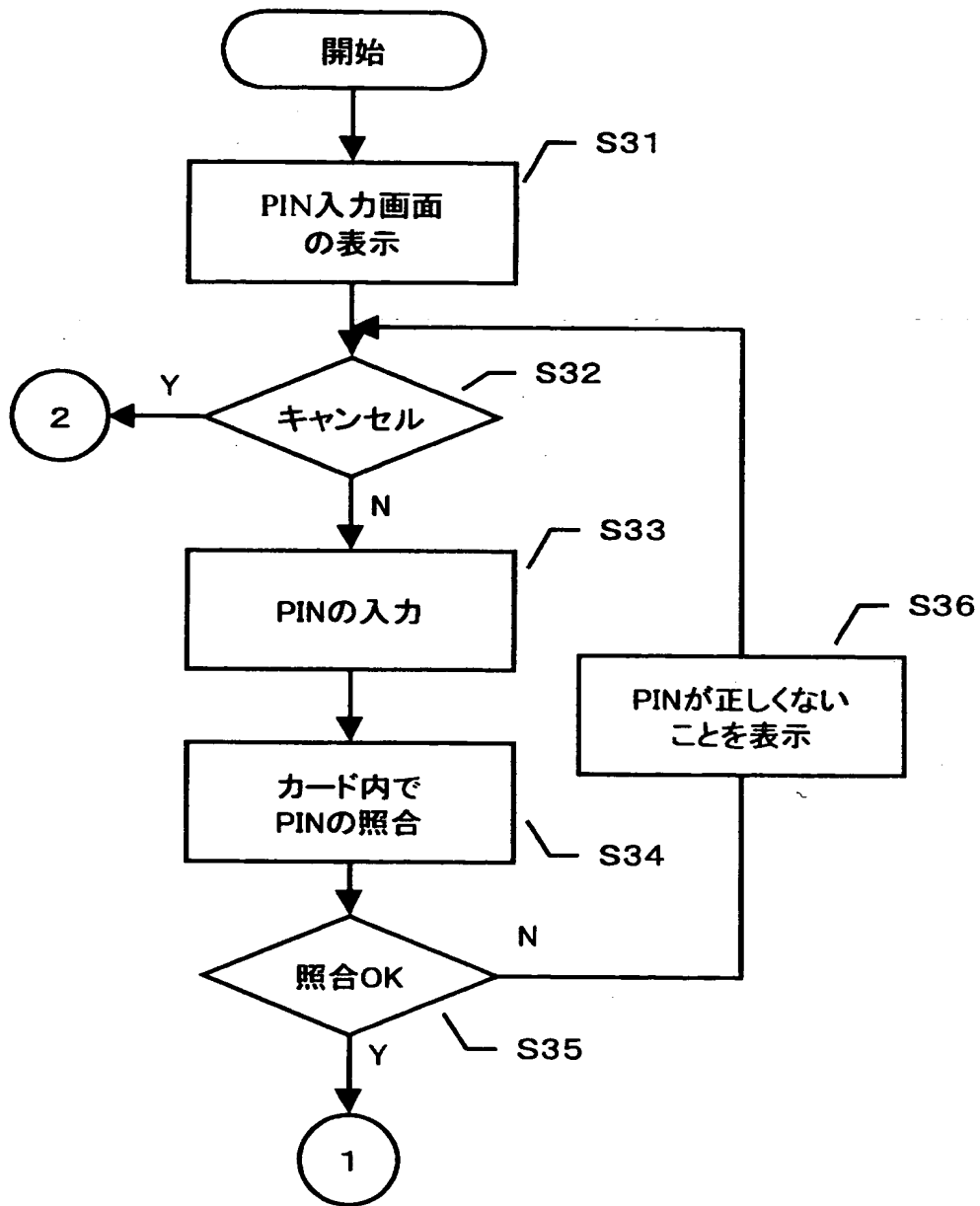
古いパスワード *****

新しいパスワード *****

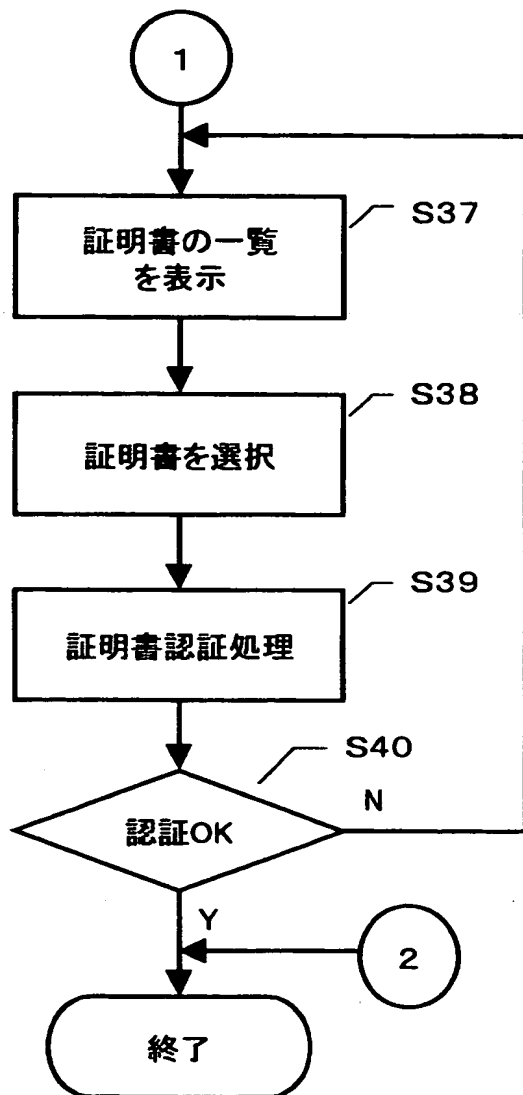
新しいパスワードの確認 *****

OK CAN

【図 10】

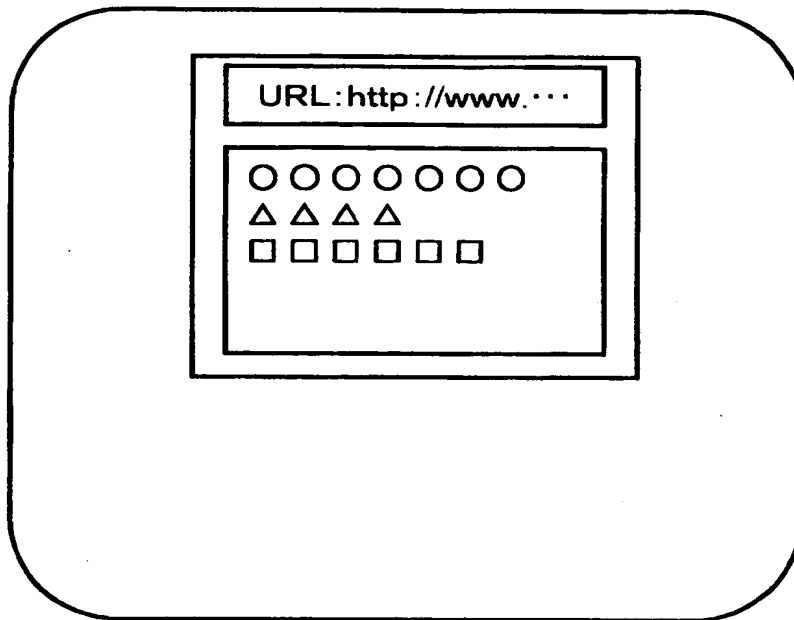


【図 1 1】

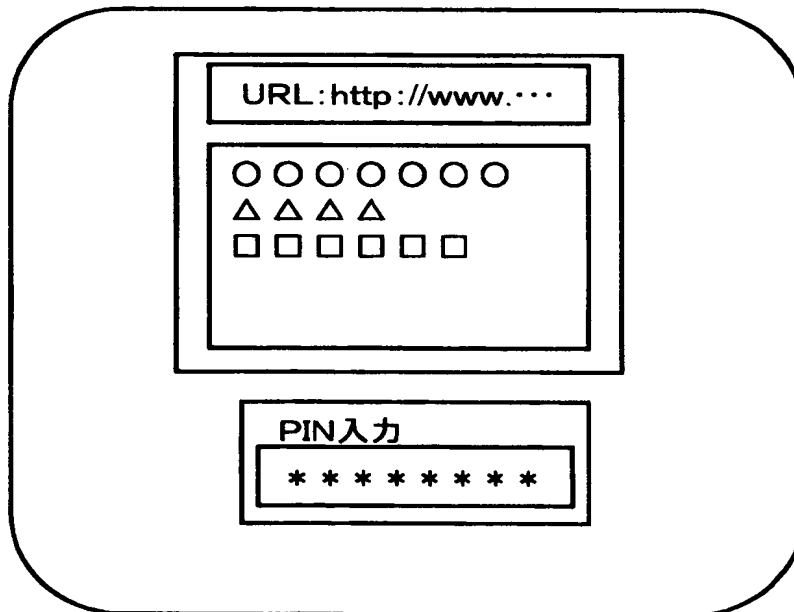


【図 12】

(a)



(b)



【図 13】

(c)

URL: http://www....

○	○	○	○	○	○	○
△	△	△	△			
□	□	□	□	□	□	□

選択してください。

☒ 証明書1

☐ 証明書2

(d)

URL: http://www....

●	●	●				
▲	▲					
■	■	■	■	■	■	■

【図 14】

アプリケーションID	ユーザID	パスワード	ドメイン	拡張
------------	-------	-------	------	----

【書類名】 要約書

【要約】

【課題】 本発明は、複数のシステムに対する利用者の操作の簡易化、複数のシステムを利用する環境におけるセキュリティ向上のための認証制御装置、認証制御システム、記録媒体を提供する。

【解決手段】 利用者により入力される入力識別情報と記録媒体に記録されている固有の識別情報とを照合し、前記照合結果に応じて、前記記録媒体に記録されている複数のシステムにそれぞれ対応する認証情報のうち対象システムに関する認証情報を読み出し、前記読み出された認証情報を認証処理の入力情報として設定する。

【選択図】 図 3

出 願 人 履 歴 情 報

識別番号 [000005223]

1. 変更年月日	1996年 3月26日
[変更理由]	住所変更
住 所	神奈川県川崎市中原区上小田中4丁目1番1号
氏 名	富士通株式会社